REMARKS

Applicant notes with appreciation the withdrawal in paragraph 3 of the present Office Action of the previous rejection in view of U.S. Patent No. 6,704,868 to *Challener et al.*

In paragraph 5 of the present Office Action, Claims 1-3, 6-11, 14-19, and 22-24 are rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,807,277 to *Doonan et al.* (*Doonan*) in view of U.S. Patent No. 6,009,177 to *Sudia*. In addition, in paragraph 6, Claims 4, 12 and 20 are rejected under 35 U.S.C. § 103 as unpatentable over *Doonan* and *Sudia* in view of U.S. Patent No. 6,732,101 to *Cook*, and in paragraph 7, Claims 5, 13 and 21 are rejected under 35 U.S.C. § 103 as unpatentable over *Doonan* and *Sudia* in view of U.S. Patent No. 4,888,800 to *Marshall*. Those rejections are respectfully traversed, and favorable reconsideration of the claims is requested.

Applicant respectfully submits that the combination of *Doonan* and *Sudia* does not render exemplary Claim 1 (and similar Claims 9 and 17) of the present invention unpatentable under 35 U.S.C. § 103 because the combination of cited references does not disclose each feature recited therein. For example, the combination of *Doonan* and *Sudia* does not disclose the following steps of exemplary Claim 1:

> storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key;
>
> ...
>
> thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system.

With respect to the claimed "associated key", page 3 of the present Office Action cites col. 5, lines 63-67 of *Doonan*, which disclose:

> The composite message P is first encrypted to form encrypted message Pe, using a randomly-generated symmetric encryption key Ks. The symmetric key Ks is then itself encrypted using the public key published in a digital certificate owned by the recipient, to form [the encrypted symmetric key] Kp. (emphasis supplied)

Thus, *Doonan's* public key of the message recipient is relied upon in the present rejection as disclosing the claimed "associated key." Under this mapping of elements, obviousness is only established if the combination of cited references disclose (in the words of Claim 1), "preventing validation of the association of the user with messages by revoking" the public key of the message recipient at the encrypting data processing system.

With reference to the step of "preventing validation of the association of the user with messages", page 4 of the present Office Action correctly notes that *Doonan* does not disclose revocation of an associated key as claimed. However, the Office Action then relies upon *Sudia's* disclosure of the conventional revocation of a key by a certifying authority at col. 22, lines 51--63:

> Whenever any user, entity or device "verifies" a digitally signed "certificate," whether a manufacturer's certificate or an escrow certificate, issued by a certifying authority or manufacturer, it is common practice in most or all actual and proposed public key certificate management systems (and it is assumed throughout this disclosure) that the user, entity or device also checks any applicable "certificate revocation list" ("CRL") in order to determine whether the certifying authority or other issuer has distributed, propagated or otherwise made available a list of revoked certificates that is updated in accord with an appropriate security policy and whether, based upon the issuer name and certificate number, the certificate has been revoked. A certificate issued to a user

The combination of *Doonan* and *Sudia* urged by the Examiner thus discloses the revocation of the message recipient's public key by the publication on a certificate revocation list (CRL) of the message recipient's certificate.

As should be apparent, the disclosure of the *Doonan* and *Sudia* relied upon by the Examiner does not teach or suggest "thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system", as recited in Claim 1. First, and most importantly, the revocation of a message recipient's public key does not "prevent[] validation of the association of the user with messages." As explained in the present specification at page 4, line 16 *et seq.*,

> If a user is no longer permitted to use a key, the certificate issuer needs to revoke the certificate for the user's key by publishing the certificate for the key on a certificate revocation list ("CRL"). However, a time gap typically exists between when a certificate issuer receives a notification that a certificate for a key should be revoked and when the certificate issuer publishes the certificate of the key on the next CRL. This time gap results in what is known as the CRL time-granularity problem. During this time period, the user may attempt to use the key to engage in unauthorized transactions and communications that should have been invalidated by the revocation of the key and the certificate for the key. The user may then continue to sign messages and communicate without proper authority. The present invention recognizes the need and desire to resolve this problem.

The publication of the certificate of a message recipient (i.e., not that the claimed "user") on the CRL does nothing to "prevent[] validation of the association of the user with messages" as claimed.

Second, the publication of message recipient's certificate on the CRL by the certificate issuer (as urged by the Examiner) does not "prevent[] validation of the association of the user with messages by revoking the associated key at the encrypting data processing system," (emphasis supplied) as claimed. That is, the publication of a message recipient's certificate on the CRL at a certificate issuer does not revoke "an associated key" at the encrypting data processing system that originates the messages.

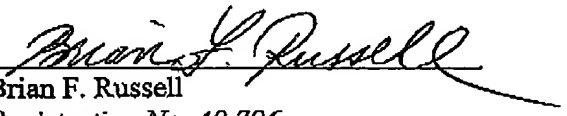
In view of the failure of the combination of *Doonan* and *Sudia* to disclose each feature recited in exemplary Claim 1, and in particular, the claimed use and revocation of an associated key at an encrypting data processing system, Applicant respectfully submits that Claim 1, similar Claims 9 and 17 and their respective dependent claims are not rendered unpatentable under 35 U.S.C. § 103.

If the Examiner harbors any lingering doubt as to the patentability of the present claims in view of the cited combination of references, Applicant hereby offers to submit a declaration swearing back of *Doonan*.

Having now responded to each rejection set forth in the present Office Action, Applicant believes all pending claims are now in condition for allowance and respectfully requests such allowance.

No additional fee is believed to be required; in the event any additional fee is required, please charge such fee to IBM Corporation Deposit Account No. **50-0563**.

Respectfully submitted,



Brian F. Russell
Registration No. 40,796
DILLON & YUDELL LLP
8911 N. Capital of Texas Hwy., Suite 2110
Austin, Texas 78759
(512) 343-6116
ATTORNEY FOR APPLICANT